



Release Notes for Cisco RF Switch Firmware Version 4.0

March 31, 2011

Cisco RF Switch Firmware Version 4.0

OL-15753-03

These release notes for the Cisco RF Switch Firmware describe the enhancements, versions, and application of the Cisco RF Switch, through Firmware Version 4.0. This document supports commands and features in prior versions of Cisco RF Switch Firmware. Firmware Version 4.0 remains subject to the restrictions and support for the N+1 Redundancy feature in Cisco IOS 12.3 BC release train.

For a list of general software configuration and operation procedures that are used for Cisco RF Switch Firmware Version 4.0 or prior, see the following document located on Cisco.com:

- *Cisco RF Switch Firmware Configuration Guide, Version 4.0*
http://www.cisco.com/en/US/products/hw/cable/ps2929/products_installation_and_configuration_guides_list.html

For a list of general software commands and operation procedures that are used for Cisco RF Switch Firmware Version 4.0 or prior, see the following document located on Cisco.com:

- *Cisco RF Switch Firmware Command Reference Guide, Version 4.0*
http://www.cisco.com/en/US/products/hw/cable/ps2929/prod_command_reference_list.html

For detailed configuration and operation procedures that apply to HCCP N+1 Redundancy on the Cisco CMTS, see the following document located on Cisco.com:

- *N+1 Redundancy for the Cisco CMTS*
<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html>

For a list of the software enhancements or caveats that apply to Cisco IOS Release 12.3 BC, see the following document located on Cisco.com:

- *Release Notes for Cisco IOS Software Release 12.3 BC*
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_release_notes_list.html



Note

You can find the most current Cisco IOS documentation on Cisco.com. This set of electronic documents may contain updates and modifications made after this document was initially published.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected.

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

Contents

These release notes describe the following topics:

- [Prerequisites for Firmware Version 4.0](#)
- [Restrictions for Firmware Version 4.0](#)
- [Prerequisites for Firmware Version 3.93](#)
- [Restrictions for Firmware Version 3.93](#)
- [Prerequisites for Firmware Version 3.92](#)
- [Restrictions for Firmware Version 3.92](#)
- [Prerequisites for Firmware Version 3.90](#)
- [Restrictions for Firmware Version 3.90](#)
- [Prerequisites for Firmware Version 3.80](#)
- [Restrictions for Firmware Version 3.80](#)
- [Prerequisites for Firmware Version 3.60](#)
- [Restrictions for Firmware Version 3.60](#)
- [Information About Cisco RF Switch Firmware Versions and Features](#)
- [Installing Cisco RF Switch Firmware Version 4.0](#)
- [Installing Cisco RF Switch Firmware Version 3.93](#)
- [Additional References](#)

Prerequisites for Firmware Version 4.0

This section describes prerequisites that apply specifically to Firmware Version 4.0 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the [“Additional References” section on page 15](#).

The following table indicates the Factory Default Image for the Ethernet cards:

Description	Part Number	Factory Default Image
Chassis with 10BaseT Ethernet Card	74-2621-03	3.92
10BaseT Ethernet Card	74-2620-01	

Restrictions for Firmware Version 4.0

This section describes restrictions that apply specifically to Firmware Version 4.0 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- Cisco recommends upgrading to Firmware Version 4.0, even with earlier Cisco IOS releases subject to N+1 Prerequisites and Restrictions such as feature interoperability, factory default configurations, etc.

Refer to the following document located on Cisco.com for further information on Cisco IOS releases:

Release Notes for Cisco IOS Software Release 12.3 BC

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_release_notes_list.html

- Upgrades should be done via tftp download, as done in previous releases. This is the first release to use the combined binary image file format.

When the RF switch recognizes the download of a combined image file, it scans the file looking for the appropriate section of the image file that applies to it. The RF switch stores the section of the download that applies to the card onto which it is loading.

- The 10BaseT Ethernet card supports only 10Mbps operation.

Prerequisites for Firmware Version 3.93

This section describes prerequisites that apply specifically to Firmware Version 3.93 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the [“Additional References” section on page 15](#).

Restrictions for Firmware Version 3.93

This section describes restrictions that apply specifically to Firmware Version 3.93 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- This version can be downloaded only on 10BaseT ethernet cards.
- This version adds support for the new Version 4 combined binary file downloads.

This version still supports the single image formats used with the earlier cards.

Prerequisites for Firmware Version 3.92

This section describes prerequisites that apply specifically to Firmware Version 3.92 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the [“Additional References” section on page 15](#).

Restrictions for Firmware Version 3.92

This section describes restrictions that apply specifically to Firmware Version 3.92 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- Cisco recommends upgrading to Firmware Version 3.92, even with earlier Cisco IOS releases subject to N+1 Prerequisites and Restrictions such as feature interoperability, factory default configurations, etc.

Refer to the following document located on Cisco.com for further information on Firmware Version 3.92:

Release Notes for Cisco IOS Software Release 12.3 BC

http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html

- Version 3.92 allocates new nvmem location to support long passwords (32 characters) and SNMP community string (64 characters).
- In Version 3.92, on first reboot after migration from previous version, the new password and community string areas are installed and old settings (if any) are copied to new location.
- **If the user downgrades from 3.92 to a previous version, some of the configuration parameters in the newer versions are not recognized by the older software which causes the some of the config elements to be reset to default values.**
- **If user downgrades from Version 3.92 to Version 3.80, the new nvmem location for password and community string is not recognized, and the password is removed and community string is set to private.**
- **If the user downgrades from Version 3.92 to Version 3.60 or earlier, the password is removed and community string is set to private, and the ip address, default gateway and tftp address are reset to default values.**



Note

Version 3.92 is case-sensitive and stores passwords and SNMP community strings as they are entered on the CLI. In previous versions the case-sensitivity was not preserved and passwords and community strings were converted internally — passwords were stored in all uppercase and community strings in all lowercase. The parser allowed the user to type in any case as long as the letters matched.

When the user upgrades to version 3.92, the mixed case passwords and SNMP community strings from previous versions are stored as lower case characters. After the upgrade, the user should verify the password and community string and set them as desired.

Prerequisites for Firmware Version 3.90

This section describes prerequisites that apply specifically to Firmware Version 3.90 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the [“Additional References” section on page 15](#).

Restrictions for Firmware Version 3.90

This section describes restrictions that apply specifically to Firmware Version 3.90 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- Cisco recommends upgrading to Firmware Version 3.90, even with earlier Cisco IOS releases subject to N+1 Prerequisites and Restrictions such as feature interoperability, factory default configurations, etc.

Refer to the following document located on Cisco.com for further information on Firmware Version 3.90:

Release Notes for Cisco IOS Software Release 12.3 BC

http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html

Prerequisites for Firmware Version 3.80

This section describes prerequisites that apply specifically to Firmware Version 3.80 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the “[Additional References](#)” section on page 15.
- The password on the RF Switch should be removed before upgrading the RF Switch to 3.80. The password can be set on the RF Switch when the upgrade to version 3.80 is complete.

Restrictions for Firmware Version 3.80

This section describes restrictions that apply specifically to Firmware Version 3.80 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- Cisco recommends upgrading to Firmware Version 3.80, even with earlier Cisco IOS releases subject to N+1 Prerequisites and Restrictions such as feature interoperability, factory default configurations, etc.

Refer to the following document located on Cisco.com for further information on Firmware Version 3.80:

Release Notes for Cisco IOS Software Release 12.3 BC

http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html

Prerequisites for Firmware Version 3.60

This section describes prerequisites that apply specifically to Firmware Version 3.60 on the Cisco RF Switch, used in conjunction with the Cisco IOS N+1 Redundancy feature on the Cisco CMTS.

- The Cisco RF Switch must be cabled and installed in full compliance with the documents listed in the “[Additional References](#)” section on page 15.
- Cisco recommends that the RF Switch Firmware be upgraded to Version 3.60 from previous Firmware versions, particularly for operation of the Cisco uBR10012 router with Cisco IOS Release 12.3(21)BC in N+1 Redundancy. Refer to general field notices, and the following documents for additional information:
 - *Field Notice: FN - 62695 - Cisco RF Switch Firmware Version 3.60 - Mandatory Upgrade, Document ID: 82266*
http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_field_notices_list.html
 - *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC*
http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html

Restrictions for Firmware Version 3.60

- Cisco recommends upgrading to Firmware Version 3.60, even with earlier Cisco IOS releases, subject to N+1 Prerequisites and Restrictions in the Cisco IOS release, such as feature interoperability, factory default configurations, and so forth.
- Refer to the following Firmware Upgrade Field Notice for additional information:
 - *Field Notice: FN - 62695 - Cisco RF Switch Firmware Version 3.60 - Mandatory Upgrade, Document ID: 82266*
http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_field_notices_list.html

Information About Cisco RF Switch Firmware Versions and Features

This topic summarizes the new commands and features for the following Firmware Versions:

- [Features Introduced in Cisco RF Switch Firmware Version 4.0, page 6](#)
- [Features Introduced in Cisco RF Switch Firmware Version 3.93, page 7](#)
- [Features Introduced in Cisco RF Switch Firmware Version 3.92, page 7](#)
- [Features Introduced in Cisco RF Switch Firmware Version 3.90, page 8](#)
- [Features Introduced in Cisco RF Switch Firmware Version 3.80, page 8](#)
- [Features Introduced in Cisco RF Switch Firmware Version 3.60, page 9](#)
- [Features Introduced in Cisco RF Switch Firmware Version 3.50, page 10](#)
- [Features Introduced in Cisco RF Switch Firmware Version 3.30, page 10](#)
- [Features Introduced in Cisco RF Switch Firmware Version 2.50, page 11](#)

Features Introduced in Cisco RF Switch Firmware Version 4.0

- Version 4.0 is the first release to use the combined binary image file format.

The new image file is:

1935001303a.bin — combined image format

When the RF switch recognizes the download of a combined image file, it scans the file looking for the appropriate section of the image file that applies to it. The RF switch stores the section of the download that applies to the card onto which it is loading.

Upgrades should be done via tftp download, as done in previous releases.

- Version 4.0 is released on the top of version 3.93, and incorporates all of the features and bug fixes of 3.93 release.
- Version 4.0 adds the following CLI command:
 - **show port**

The 10BaseT Ethernet card supports only 10Mbps operation.

Features Introduced in Cisco RF Switch Firmware Version 3.93

Version 3.93 adds support for the new Version 4.0 combined binary file downloads. This version still supports the single image formats used with the earlier cards.

Fixes for Firmware Version 3.93:

- There was an error in the SHOW MODULE command that was generating incorrect status display for the last module.
- The DHCP client was sending out an ARP request to 0.0.0.0, when there was a need to check if the offered address was in use.
- Adjusted TFTP timeouts. The initial timeout when trying to establish a connection to the server could be too short, as it was randomly generated. Now, a minimum timeout of 1second is enforced.
- Added display of the MAC address to the bootup process.

Features Introduced in Cisco RF Switch Firmware Version 3.92

Cisco RF Switch Firmware Version 3.92 provides the following changes, resolutions, enhancements, and updates, supported on the Cisco uBR10012 router with Cisco IOS release 12.3(21)BC or later:

- Version 3.92 allocates new nvram location to support long passwords (up to 32 characters) and SNMP community strings (up to 64 characters).
- Version 3.92 stores passwords and SNMP community strings the way they are entered on the CLI. The user can store mixed case strings for passwords and SNMP community strings. In previous versions, passwords were stored in all uppercase and SNMP community strings were stored in all lowercase.
- In Version 3.92, password and SNMP community strings may contain any of the printable ASCII characters (0x20-0x7e), with the exception of the space (0x20), double quote (0x22), semicolon (0x3b), backslash (\), and forward slash (/) characters. In addition the character '?' and 'HELP' cannot be used in strings by themselves as they invoke the CLI help function.
- In Version 3.92, on first reboot after migration from previous version, the new password and community string areas are installed and old settings (if any) are copied to new location. If the user moves to a previous version from 3.92, the password is removed and community string is set to **private**.

- Version 3.92 enhances the command **show log** and it now includes the nvram status message entries.
- Version 3.92 introduces **show password help**.
- Version 3.92 added **reload/reboot** and **reload?** to the main help.
- Version 3.92 enhances **enable password** and **set snmp community** help and it now lists characters not recommended in these strings.

Features Introduced in Cisco RF Switch Firmware Version 3.90

Cisco RF Switch Firmware Version 3.90 provides the following changes, resolutions, enhancements, and updates, supported on the Cisco uBR10012 router with Cisco IOS release 12.3(21)BC or later:

- Version 3.90 update resolves the Address Resolution Protocol (ARP) cache handling issue and ensures ARP updates after timeout.
- Version 3.90 provides for enhancement in the telnet server to negotiate with the client regarding the desired setting of the echo mode. The user can set the initial state of the local echoing using the **set telnet echo** command. However, the telnet server can bypass this and use the client's setting if the client supports echo options negotiation.
- Version 3.90 enhances the Trivial File Transfer Protocol (TFTP) to display the number of bytes as transfer progresses.
- Version 3.90 pushes the CLI task priority to below that of the network task. Now, pings have higher priority than interface commands.
- Version 3.90 modifies the command **show version** so that the full cyclic redundancy check (CRC) validation is not done on the flash contents. It now validates only the file header contents. To perform a full CRC check, use the command **show files**.
- Version 3.90 allows RF Switch to accept passwords that match CLI keywords. In version 3.80, they were not accepted and shown as Invalid Syntax.
- Version 3.90 updates real-time operating system (RTOS) kernel to be compatible with new IP stack.

Features Introduced in Cisco RF Switch Firmware Version 3.80

Cisco RF Switch Firmware Version 3.80 provides the following changes, resolutions, enhancements, and updates, supported on the Cisco uBR10012 router with Cisco IOS release 12.3(21)BC or later:

- Version 3.80 adds the **set access system** command. This command is similar to the **password system** command, which is no longer valid in Version 3.80 or later. The **set access system** command enables access to commands that were previously available only via backdoor password. This command works in addition to any installed password, and does not override any current password protection.
- Version 3.80 adds the **set** option to the **show config** command, enabling you to display the config information formatted as SET commands.
- Version 3.80 introduces a new password recovery procedure.
- Version 3.80 adds an *all* option to the **show switch status** command. This enables users to display detailed RF Switch status for all modules (1-28), including the last command used, the detected module position, and any relays that are in error.

- Version 3.80 fixes the telnet mode so that typing the **quit** or **exit** command in a telnet session will cause the rfsw telnet server to close the connection.
- Version 3.80 adds an *echo* option negotiation to the rfsw telnet server. The new **set telnet echo** command sets the default state for echoing in the rfsw telnet server. To restore the default state, use the **no** form of the command.
- Version 3.80 adds the **enable** command. Using the **enable** command in user EXEC mode enables the user to enter privileged exec mode.
- In Version 3.80, the command **enable erase** is changed to **allow erase**. This command helps to prevent accidental image erasure.
- Version 3.80 adds the **enable password** command. This command sets enable mode password and store it in nvram. To remove the password requirement, use the **no** form of this command.
- Version 3.80 adds the **disable** command. This command exits privileged EXEC mode and return to user EXEC mode, or to exit to a lower privilege level, enter the disable command in EXEC mode.
- Version 3.80 adds caching of snmp mib vars to the AdminState sets/gets.
- Version 3.80 adds a new mib oid to control caching.

Features Introduced in Cisco RF Switch Firmware Version 3.60

Cisco RF Switch Firmware Version 3.60 provides the following changes, resolutions, enhancements, and updates, supported on the Cisco uBR10012 router with Cisco IOS release 12.3(21)BC or later:

- To help handle an increase in the SNMP traffic, Version 3.60 changes the network buffering to allocate a larger pool of (number of) buffers, with a new number of 100 buffers total.
- Version 3.60 reduces the maximum packet size to 600 bytes. This combination of a larger number of buffers with smaller maximum packet size helps with handling large bursts of inbound packets that were discarded in previous versions of Cisco RF Switch Firmware.
- Version 3.60 resolves a previous bug in the SNMP agent to help further with the above items. In prior versions of Cisco RF Switch firmware, the SNMP agent blocked traffic just after packet reception, waiting to allocate a buffer in which to place the output response. If no buffer was available (as would be the case if a large burst of incoming packets occurred), the agent would timeout, and the system would generate a watchdog timeout. Now, the agent uses a private buffer for the output response, and only requests a packet buffer after completing the snmp operation. If no buffer is available, the output response is discarded, and the agent continues processing inbound packets.
- Version 3.60 adds the **noverify** option to the **copy** command, enabling you to override the file type verification, and place a file in either the flash (FL:) or bootflash (BF:) device. Version 3.60 updates the online help to reflect this new option. This new option provides the ability to place a copy of the main application into the bootflash, so that normal system operation is restarted in the case of a system crash, instead of having the “sys>” prompt as in previous versions of Firmware.
- Version 3.60 resolves a previous issue in which concurrent access to the RF switch modules via the command-line interface and SNMP would cause random errors and crashes. The firmware now allows simultaneous usage of telnet, console, and SNMP operation. This issue was observed primarily if the show version and test module commands were used at the same time that SNMP status polling operations were occurring. This previous issue also affected a number of additional commands.

Features Introduced in Cisco RF Switch Firmware Version 3.50

Firmware Version 3.50 can be used with either Cisco IOS Release 12.2(15)BC1 or 12.2(15)BC2 for full availability of improved switchover times.

Improved Switchover Times

Firmware Versions 3.30 and 3.50 both offer significantly improved switchover times in the event of a Working interface or line card failure. Also, N+1 Redundancy is more easily configured with increased synchronization between Working and Protect interfaces. Refer to *N+1 Redundancy for the Cisco Cable Modem Termination System* on Cisco.com:

ARP Cache

Firmware Version 3.50 modifies Address Resolution Protocol (ARP) cache functions to reduce the number of ARP requests as possible. The ARP timeout was previously fixed at 60 seconds. This is now a definable setting from the RF Switch command-line interface (CLI). Commands relating to ARP are described later in this section.

Cisco Command Changes for Firmware Version 3.50

Version 3.50 offers the following command enhancements, continued through Version 3.60:

- Added the new **set arp timeout** command to allow configuration of the ARP cache feature (see above).
- Enhanced the **show config** command to display ARP timeout information.
- Enhanced the **show arp** command. There are now three forms:
 - **show arp** — Displays minimal information to show valid entries in use.
 - **show arp all** — Displays more details, including link-list information and entries that may be expired.
 - **show arp table** — Displays full table, including unused entries.

Features Introduced in Cisco RF Switch Firmware Version 3.30

Firmware Version 3.30 can be used with either Cisco IOS Release 12.2(15)BC1 or 12.2(15)BC2 for full availability of improved switchover times.

Improved Switchover Times

Firmware Versions 3.30 and 3.50 both offer significantly improved switchover times in the event of a Working interface or line card failure. Also, N+1 Redundancy is more easily configured with increased synchronization between Working and Protect interfaces. Refer to the following document on Cisco.com for additional information:

- *N+1 Redundancy for the Cisco Cable Modem Termination System* on Cisco.com:
<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html>

Firmware Command Changes for Version 3.30

Version 3.30 offers the following command enhancements, continued through Version 3.60:

- Replaces the **configure card count** command with the **set slot config** command for setting Cisco RF Switch slots to line cards on the router chassis.

Previously, Version 2.50 required that upstream and downstream line cards be configured to specific slots in the RF Switch chassis (using the **configure card count** command). Firmware Version 3.30 allows for the RF Switch chassis to be configured with any mix of upstream or downstream line cards using the **set slot config** command.

- Adds the **show ip** command to display IP configuration information for the Cisco RF Switch.
- Adds display of slot configuration information with the **show slot config** command.
- Modifies the `password` field output displayed in the **show config** Firmware command so as to preserve password security with encryption.
- Modifies the `Card Protect Mode` field output in the **show config** command to change the previous notations of 1x4/1x8 to the Cisco standard notations of 4+1/8+1.

DHCP Server added for Firmware Version 3.30

Version 3.30 adds support for the DHCP server and the DHCP client, and the RF Switch Firmware no longer assumes a static IP address of 10.0.0.1 as in Version 2.50.

Features Introduced in Cisco RF Switch Firmware Version 2.50

SNMPv1 Upconverters and Traps

Version 2.50 introduces support for the Cisco 3x10 RF Switch and SNMP upconverters with the Cisco uBR10012 router. Firmware Version 2.50 fully implements SNMPv1 and Traps. SNMP traps are sent with the following events:

- System startup (coldstart)
- Whenever the N+1 Redundancy Unit (NRU) has completed initialization:
 - `nruModuleOnOffNotification` and/or `nruModuleFaultNotification`
- Whenever a switchover fails:
 - `nruModuleFaultNotification`
- Whenever a system crash is detected:
 - `nruModuleOnOffNotification.999 offline`

Because the system remains largely inactive unless a switchover is requested, the controller (after startup) is not able to detect a cable interface line card that is removed or has failed until told to perform some action. The controller automatically detects a line card that is inserted into the chassis. Therefore, you get automatic notification if a line card is replaced.

Default Gateway for Remote TFTP Transfer

Version 2.50 adds support for the default gateway to enable TFTP transfers of remote Firmware images.

Installing Cisco RF Switch Firmware Version 4.0

As with previous Firmware upgrades on the Cisco RF Switch, the new Version 4.0 image can be downloaded and installed via TFTP using the `COPY TFTP:` command. This command can be applied from either the serial console port or a via a Telnet session.

One recommended procedure for installing the upgrade is as follows:

- Step 1** Copy the image to CMTS:
COPY TFTP://<tftpserver-ip>/<userid>/1935001303a.bin BOOTFLASH:
- Step 2** Setup the tftp server on CMTS:
CONF T
TFTP-SERVER BOOTFLASH:1935001303a.bin ALIAS 1935001303a.bin
END
- Step 3** Setup RF Switch with tftp host, if not already set:
SET TFTP HOST <tftpserver-ip-addr>
- Step 4** Remove the password that has been set on the RF Switch, only if you are loading Version 3.80:
 The CLI to remove password in Version 3.80 or later is:
NO ENABLE PASSWORD
 The CLI to remove password in versions prior to 3.80 is:
NO SET PASSWORD
- Step 5** Install the new code update with the following command:
COPY TFTP:1935001303a.bin FLASH:
- Step 6** Reboot the Cisco RF Switch to run the new version of firmware:
REBOOT
- Step 7** Go to the enable prompt:
ENABLE
- Step 8** Install the new firmware image into the bootflash: using the new COPY command:
COPY TFTP:1935001303a.bin BOOTFLASH: NOVERIFY
- Step 9** Reboot the Cisco RF Switch to run the new version of firmware:
RELOAD
 A sample output of the reload command is given below:

```

rfs witch#reload

Nru Rom Monitor V1.10
Firmware: 1935033   Nov 12 2001,15:15:38

Locating boot device...AMD 29F400T (128k bytes)
Locating flash device...AMD 29F016 (4096k bytes)

Watchdog Reg: 0xc080
ResetCfg Reg: 0x00

Validating bootflash: contents...ok. status (0,0)
Validating flash: contents...ok. status (0,0)

Opening flash:...
Loading...

Weinschel uBR-RFSW Rfs witch CLI V400r3A
Firmware: 1935001301a   Aug 19 2008

Init hardware...
Running selftest...ok
Locating FlashFile...AMD 29F016 (4096k bytes)
    
```

```

Creating system resources...

Recalling nvmem...ok
Initializing linecard controller...
Chassis configuration: 10 upstream/3 dnstream linecards
Enumerating linecards... 13 card(s) found

MAC addr: 00:03:8F:01:04:41
Installing network stack...
Initializing network interface...IP addr: 2.41.28.30
Setting gateway addr: 2.48.28.20
Installing Telnet server...
Installing SNMP agent...

System initialization completed.

```

- Step 10** Set the password back on the RF Switch if you had removed it before upgrade. In Version 3.80 and later, the CLI to set enable password is:

```
ENABLE PASSWORD <password>
```

show version and **show log** commands help you check the upgrade. The Commands along with the RF Switch output are given below:

```
rfswitch>show version
```

```

Controller firmware:
  RomMon: 1935033 V1.10
  Bootflash: 1935001301a V400r3A
  Flash: 1935001301a V400r3A
<---- Output snipped---->

```

```
rfswitch>show log
history log has 55 entries
```

```

      Timestamp    Code  Message
0:00:37.955      0  log cleared
0:01:23.910      0  TFTP download started
0:02:31.145      0  TFTP operation completed
0:03:20.000      0  TFTP download started
0:04:24.530      0  TFTP operation completed
0:05:12.600      0  cli generating reboot
0:00:00.000      0  ** BOOT EVENT** main application booting
0:00:00.000      0  Running selftest...
0:00:00.000      0  Creating system resources
0:00:00.065      0  initializing application
0:00:00.135      0  Initializing linecard controller...

```

```
<---- Output snipped---->
```

This procedure is subject to the changes and additional restrictions applied by the Field Notice in the following document on Cisco.com:

- *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC*
http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html

Installing Cisco RF Switch Firmware Version 3.93

As with previous Firmware upgrades on the Cisco RF Switch, the new Version 3.93 image can be downloaded and installed via TFTP using the COPY TFTP: command. This command can be applied from either the serial console port or a via a Telnet session.



Note

This version can be downloaded only on the 10BaseT ethernet card.

One recommended procedure for installing the upgrade is as follows:

Step 1 Copy the image to CMTS:

COPY TFTP: //<tftpserver-ip>/<userid>/rfs_w_v393.bin BOOTFLASH:

Step 2 Setup the tftp server on CMTS:

```
CONF T
TFTP-SERVER BOOTFLASH:rfs_w_v393.bin ALIAS rfs_w_v393.bin
END
```

Step 3 Setup RF Switch with tftp host, if not already set:

```
SET TFTP HOST <tftpserver-ip-addr>
```

Step 4 Remove the password that has been set on the RF Switch, only if you are loading Version 3.80:

The CLI to remove password in Version 3.80 or later is:

```
NO ENABLE PASSWORD
```

The CLI to remove password in versions prior to 3.80 is:

```
NO SET PASSWORD
```

Step 5 Install the new code update with the following command:

```
COPY TFTP:rfs_w_v393.bin FLASH:
```

Step 6 Reboot the Cisco RF Switch to run the new version of firmware:

```
REBOOT
```

Step 7 Go to the enable prompt:

```
ENABLE
```

Step 8 Install the new firmware image into the bootflash: using the new COPY command:

```
COPY TFTP:rfs_w_v393.bin BOOTFLASH: NOVERIFY
```

Step 9 Reboot the Cisco RF Switch to run the new version of firmware:

```
REBOOT
```

While rebooting, the console displays the following warning message to show that changes have been made to nvmem:

```
Recalling nvmem... ** nvmem default(s) used (0x0c) **
**WARNING** The following non-volatile configuration memory area(s)
**WARNING** have been modified or updated:
Ethernet/IP
SNMP
```

Step 10 Set the password back on the RF Switch if you had removed it before upgrade. In Version 3.80 and later, the CLI to set enable password is:

ENABLE PASSWORD <password>

show version and **show log** commands help you check the upgrade. The Commands along with the RF Switch output are given below:

```

rfswitch>show version

Controller firmware:
  RomMon: 1935033 V1.10
  Bootflash: 1935030p V393r1
  Flash: 1935030p V393r1
<----- Output snipped ----->

rfswitch> show log
history log has 63 entries

      Timestamp      Code    Message
1755:08:05.715      0    log cleared
1755:08:15.180      0    TFTP download started
1755:09:02.315      0    Warning : idle task is unable to run
1755:09:07.060      0    TFTP operation completed
1755:09:24.955      0    TFTP download started
1755:10:17.340      0    TFTP operation completed
1755:10:19.595      0    cli generating reboot
  0:00:00.000      0    ** BOOT EVENT** main application booting
  0:00:00.000      0    Running selftest...
  0:00:00.000      0    Creating system resources
  0:00:00.065      0    initializing application
  0:00:00.095     -1    NVMEM: installing default PasswdCfg
  0:00:00.095     -1    NVMEM: transferring old passwd to PasswdCfg
  0:00:00.135     -1    NVMEM: removing old passwd from EnetCfg
  0:00:00.180     -1    NVMEM: installing default SnmpCommunityCfg
  0:00:00.180     -1    NVMEM: transferring old community to SnmpCommunityCfg
  0:00:00.245     -1    NVMEM: removing old community str from SnmpCfg
  0:00:00.270     12    ** nvmem default(s) used
  0:00:00.455      0    Initializing linecard controller...
<----- Output snipped ----->

```

This procedure is subject to the changes and additional restrictions applied by the Field Notice in the following document on Cisco.com:

- *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC*
http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS CMTS Cable Command Reference	<ul style="list-style-type: none"> • <i>Cisco IOS CMTS Cable Command Reference</i> http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Related Topic	Document Title
Cisco RF Switch Hardware	<ul style="list-style-type: none"> • Cisco uBR 3x10 RF Switch Documentation Guide, License and Warranty http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/roadmap/rdmp310.html • Cabling Cisco uBR 3x10 RF Switches to Cisco uBR-MC3GX60V Cable Interface Line Cards in a Cisco uBR10012 CMTS Router http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr_mc3gx60v/quick/start/3G60_cabling_qsg.html • Cabling Cisco uBR 3x10 RF Switches to Cisco uBR10-MC5X20S/U Cable Interface Line Cards in a Cisco uBR10012 CMTS http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr10_mc5x20s_u_h/quick/start/520QSC02.html • Cabling the Cisco uBR 3x10 RF Switch http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/quick/start/rfcabqsg.html • Cisco uBR 3x10 RF Switch Hardware Installation and Cabling Guide http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/installation/guide/icg.html • Rack-Mounting the Cisco uBR 3x10 RF Switch with the Cisco uBR10012 CMTS - Quick Start Guide http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/quick/start/ub10swrk.html • <i>Bitmap Calculator for N+1 Configuration with the Cisco RF Switch</i> (Microsoft Excel format) http://www.cisco.com/warp/public/109/BitMap.xls • Cisco RF Switch Product Home Page http://www.cisco.com/en/US/products/hw/cable/ps2929/tsd_products_support_series_home.html
Cisco RF Switch Firmware	<ul style="list-style-type: none"> • <i>Cisco RF Switch Firmware Command Reference Guide</i> http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/command/reference/rfswcr36.html • <i>Cisco RF Switch Firmware Configuration Guide</i> http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/configuration/guide/rfswcf36.html
Cisco uBR10012 Universal Broadband Router	<ul style="list-style-type: none"> • <i>Cisco uBR10012 Universal Broadband Router</i> Product page (complete documentation set) http://www.cisco.com/en/US/products/hw/cable/ps2209/tsd_products_support_series_home.html
Cisco uBR7200 Series Universal Broadband Routers	<ul style="list-style-type: none"> • Cisco uBR7200 Series Universal Broadband Routers Product page (complete documentation set) http://www.cisco.com/en/US/products/hw/cable/ps2217/tsd_products_support_series_home.html

Standards

The Cisco uBR10012 router and the Cisco RF Switch each support N+1 redundancy in compliance with these industry standards:

- Data-Over-Cable Service Interface Specifications (DOCSIS):
 - DOCSIS 1.0 support for end-to-end cable telecommunications
 - DOCSIS 1.1 support for end-to-end cable telecommunications
 - DOCSIS 2.0 support for end-to-end cable telecommunications
 - DOCSIS 3.0 support for end-to-end cable telecommunications
- European DOCSIS (EuroDOCSIS)
- PacketCable

Refer to the release notes for additional information about standards supported by your specific CMTS equipment.

MIBs

MIBs for Cisco RF Switch Firmware Version 3.30

Access to the chassis line card configuration via SNMP requires the addition of the following new objects to the MIB database, summarized in [Table 1](#). Each of these objects has these three attributes:

- SYNTAX: OCTET STRING (SIZE(2))
- ACCESS: read-only
- STATUS: mandatory



Note

Because these objects are 16-bit hex integer bitmasks, in keeping with the conventions currently used in other bitmask values, they are declared as OCTET STRING (SIZE(2)).

Table 1

MIBs Objects Required with Firmware Version 3.30 and Later.

Object	Description
nruCacheSnmpData	Value of set snmp cache command. A value of 1 in a bit position indicates that the caching is enabled. It is enabled by default.
nruUpstreamSlotConfig	Value of the <i>upstreamslots</i> parameter of the set slot config command. A value of 1 in a bit position indicates that the corresponding slot should expect an upstream linecard.
nruUpstreamSlotDetected	Results of line card enumeration. A value of 1 in a bit position indicates that an upstream linecard was detected in the slot. Normally, this value should equal nruUpstreamSlotConfig.
nruUpstreamSlotErrors	A value of 1 in any bit position indicates that there is a discrepancy between the configured versus the detected settings for the slot.
nruDnstreamSlotConfig	Value of the <i>dnstreamslots</i> parameter of the set slot config command. A value of 1 in a bit position indicates that the corresponding slot should expect a downstream line card.

Object	Description
nruDnstreamSlotDetected	Results of line card enumeration. A value of 1 in a bit position indicates that a downstream linecard was detected in the slot. Normally, this value should equal nruDnstreamSlotConfig.
nruDnstreamSlotErrors	A value of 1 in any bit position indicates that there is a discrepancy between the configured versus the detected settings for the slot

Additional MIB Information

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the [Cisco Network Management Software](#) web page (MIBs sections) on Cisco.com.

RFCs

No new or modified RFCs are supported by this feature.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/en/US/support/index.html

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

©2008-2011 Cisco Systems, Inc. All rights reserved.